



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11167487 A**(43) Date of publication of application: **22.06.99**

(51) Int. Cl.

G06F 9/06
G06F 13/00
G06F 13/00
G06F 15/00

(21) Application number: **09331409**(71) Applicant: **FUJITSU LTD**(22) Date of filing: **02.12.97**(72) Inventor: **NOJIRI NATSUKI**

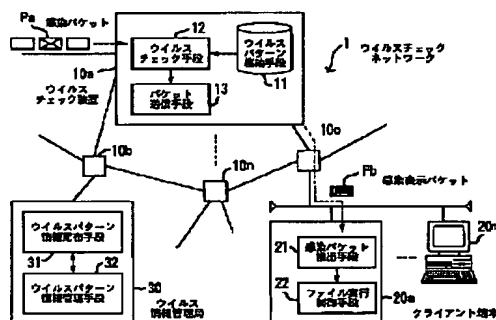
(54) **VIRUS CHECK NETWORK, VIRUS CHECK
 DEVICE, CLIENT TERMINAL AND VIRUS
 INFORMATION MANAGING STATION**

COPYRIGHT: (C)1999,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a virus check network with improved efficiency to prevent viruses on a network side.

SOLUTION: A virus pattern housing means 11 houses virus patterns. A virus check means 2 executes virus check whether a packet is an infected packet Pa or not based on the virus patterns on the network side. At the time of detecting an infected packet Pa, a packet transmitting means 13 stands a bit showing infection within the packet and transmits it as an infection displaying packet Pb. An infected packet detecting means 21 detects the infected packet. A file execution control means 22 makes a file execution-disable corresponding to the infected packet. A virus pattern information delivering means 31 delivers virus pattern information to virus check devices 10a to 10n by multicasting. A virus pattern information managing means 32 uniformly manages virus pattern information.



(51)Int.Cl.⁶

G 0 6 F 9/06
13/00
15/00

識別記号

5 5 0
3 5 1
3 5 5
3 3 0

F I

G 0 6 F 9/06
13/00
15/00

5 5 0 Z
3 5 1 Z
3 5 5
3 3 0 A

審査請求 未請求 請求項の数12 O L (全 14 頁)

(21)出願番号

特願平9-331409

(22)出願日

平成9年(1997)12月2日

(71)出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72)発明者 野尻 夏樹

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

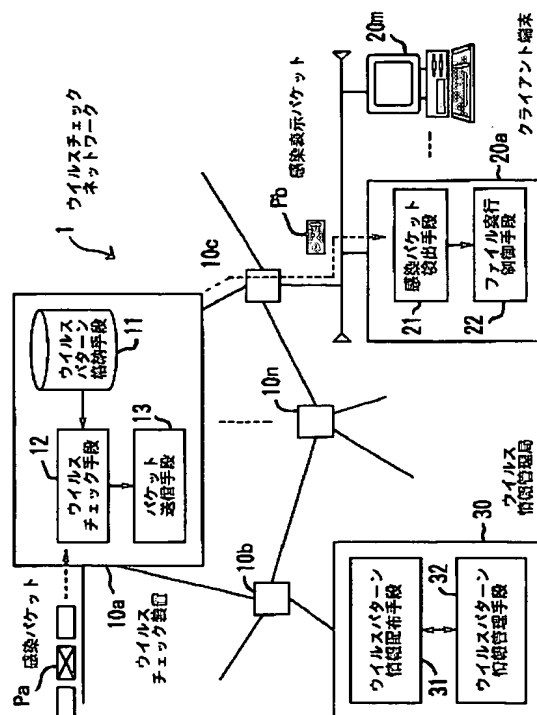
(74)代理人 弁理士 服部 毅彦

(54)【発明の名称】 ウィルスチェックネットワーク、ウィルスチェック装置、クライアント端末及びウィルス情報管理
理局

(57)【要約】

【課題】 ネットワーク側でウィルスを未然に防ぎ、ウィルス対策効率の向上を図ったウィルスチェックネットワークを提供することを目的とする。

【解決手段】 ウィルスパターン格納手段11は、ウィルスパターンを格納する。ウィルスチェック手段12は、パケットをウィルスパターンにもとづいて、感染パケットPaか否かのウィルスチェックをネットワーク側で行う。パケット送信手段13は、感染パケットPa検知時は、パケット内の感染を示すビットを立てて感染表示パケットPbとして送信する。感染パケット検出手段21は、感染パケットPaを検出する。ファイル実行制御手段22は、感染パケットに対応するファイルを実行不可にする。ウィルスパターン情報配布手段31は、ウィルスパターン情報をマルチキャストでウィルスチェック装置10a～10nに配布する。ウィルスパターン情報管理手段32はウィルスパターン情報を一元管理する。



【特許請求の範囲】

【請求項1】 ウイルスチェックを行って、ウイルス侵入を防止するウイルスチェックネットワークにおいて、ウイルスパターンを格納するウイルスパターン格納手段と、受信したパケットを前記ウイルスパターンにもとづいて、ウイルスに感染している感染パケットか否かの前記ウイルスチェックをネットワーク側で行うウイルスチェック手段と、前記感染パケットを検知した場合は、感染を示すパケット内のビットを立てて感染表示パケットとして送信するパケット送信手段と、から構成される複数のウイルスチェック装置と、前記ビットにもとづいて、前記感染パケットを検出する感染パケット検出手段と、前記感染パケットに対応するファイルを実行不可にするファイル実行制御手段と、から構成されるクライアント端末と、ウイルスパターン情報をマルチキャストで前記ウイルスチェック装置に配布するウイルスパターン情報配布手段と、前記ウイルスパターン情報を一元管理するウイルスパターン情報管理手段と、から構成されるウイルス情報管理局と、を有することを特徴とするウイルスチェックネットワーク。

【請求項2】 前記ウイルスチェック手段は、前記パケットのヘッダを見て前記ウイルスチェックすべき前記パケットを選定することを特徴とする請求項1記載のウイルスチェックネットワーク。

【請求項3】 前記ウイルスチェック装置は、ルータに配置されることを特徴とする請求項1記載のウイルスチェックネットワーク。

【請求項4】 前記ウイルスチェック装置は、前記ウイルスパターン情報を前記マルチキャストで互いに通知することを特徴とする請求項1記載のウイルスチェックネットワーク。

【請求項5】 前記ウイルスチェック装置は、前記ウイルスの脅威レベルに応じて警戒モードを設定し、ホストとの通信を一定時間遮断させる警戒モード設定手段をさらに含むことを特徴とする請求項1記載のウイルスチェックネットワーク。

【請求項6】 前記ウイルスチェック装置は、前記ウイルスチェックを行う部位を複数設け、前記ウイルスチェック装置毎に担当するウイルスチェック領域を分担することを特徴とする請求項1記載のウイルスチェックネットワーク。

【請求項7】 前記ウイルスチェック装置は、ネットワーク上新規に置かれた場合は、他の前記ウイルスチェック装置から前記ウイルスチェックの担当領域情報を収集することを特徴とする請求項6記載のウイルスチェックネットワーク。

【請求項8】 前記パケット送信手段は、前記感染表示パケットの送信と共に、前記感染パケットの送信元に警

告パケットを送信し、かつ他の前記ウイルスチェック装置に警戒すべき前記感染パケットの情報が記された警戒情報パケットをマルチキャストで配布することを特徴とする請求項1記載のウイルスチェックネットワーク。

【請求項9】 前記ウイルスチェック手段は、前記警戒情報パケットに記された前記感染パケットの前記ウイルスパターンの優先順位を上げて、前記ウイルスチェックを行うことを特徴とする請求項8記載のウイルスチェックネットワーク。

【請求項10】 ウイルスチェックを行って、ウイルス侵入を防止するウイルスチェック装置において、ウイルスパターンを格納するウイルスパターン格納手段と、

受信したパケットを前記ウイルスパターンにもとづいて、ウイルスに感染している感染パケットか否かの前記ウイルスチェックをネットワーク側で行うウイルスチェック手段と、

前記感染パケットの場合は、感染を示すパケット内のビットを立てて感染表示パケットとして送信するパケット送信手段と、

を有することを特徴するウイルスチェック装置。

【請求項11】 ウイルスチェックを受けたパケットを受信するクライアント端末において、ウイルスに感染されていることを示すビットが立っているパケットを感染パケットとして検出する感染パケット検出手段と、

前記感染パケットを検出した場合は、対応するファイルを実行不可にするファイル実行制御手段と、を有することを特徴するクライアント端末。

【請求項12】 ネットワーク内のウイルス情報を管理するウイルス情報管理局において、ウイルスパターン情報を前記ネットワーク内に配置されたウイルスチェックを行うウイルスチェック装置にマルチキャストで配布するウイルスパターン情報配布手段と、前記ウイルスパターン情報を一元管理するウイルスパターン情報管理手段と、

を有することを特徴するウイルス情報管理局。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はウイルスチェックネットワーク、ウイルスチェック装置、クライアント端末及びウイルス情報管理局に関し、特にウイルスチェックを行って、ウイルス侵入を防止するウイルスチェックネットワーク、ウイルスチェックを行って、ウイルス侵入を防止するウイルスチェック装置、ウイルスチェックを受けたパケットを受信するクライアント端末及びネットワーク内のウイルス情報を管理するウイルス情報管理局に関する。

【0002】

【従来の技術】 近年、マルチメディア通信などの情報通

信ネットワーク技術が急速に進歩している。また、インターネット等の流行により、企業のみならず一般家庭に対しても、ネットワークが提供するサービスが幅広く利用されている。

【0003】この反面、コンピュータウィルスの増加と感染のスピードは、ネットワークの普及と共に加速しており、多くの企業ユーザがウィルスの被害に遭っている現状が報告されている。

【0004】従来、ネットワークをウィルスの感染から守るには、クライアントやプロキシサーバ等にワクチン・ソフトを導入していた。このワクチン・ソフトを用いることにより、ウィルスに感染しているファイルからウィルスを取り去って、ファイルを修復することができる。

【0005】

【発明が解決しようとする課題】しかし、上記のような従来のウィルス対策は、クライアント側で行っているため、感染防止にはクライアントすべてに対して、個々にワクチン・ソフトを導入しなければならない。

【0006】このため、新種ウィルスに対しては、バージョンアップしたワクチン・ソフトを最初から逐一導入しなければならず、時間が非常にかかり効率が悪いといった問題があった。

【0007】また、従来のクライアント側でのウィルス対策では、新種ウィルス発見時のパターンファイルの更新などをはじめとする運用管理等は、各自ユーザに任せられるため、ウィルス監視を徹底させることが難しいといった問題があった。

【0008】本発明はこのような点に鑑みてなされたものであり、ネットワーク側でウィルスを未然に防ぎ、ウィルス対策効率の向上を図ったウィルスチェックネットワークを提供することを目的とする。

【0009】また、本発明の他の目的は、ネットワーク側でウィルスを未然に防ぎ、ウィルス対策効率の向上を図ったウィルスチェック装置を提供することである。さらに、本発明の他の目的は、ウィルスに感染しているファイルを削除して、ウィルス対策効率の向上を図ったクライアント端末を提供することである。

【0010】また、本発明の他の目的は、ネットワーク内のウィルス情報を管理して、ウィルス対策効率の向上を図ったウィルス情報管理局を提供することである。

【0011】

【課題を解決するための手段】本発明では上記課題を解決するために、図1に示すような、ウィルスチェックを行って、ウィルス侵入を防止するウィルスチェックネットワーク1において、ウィルスパターンを格納するウィルスパターン格納手段11と、受信したパケットをウィルスパターンにもとづいて、ウィルスに感染している感染パケットPaか否かのウィルスチェックをネットワーク側で行うウィルスチェック手段12と、感染パケット

Paを検知した場合は、感染を示すパケット内のビットを立てて感染表示パケットPbとして送信するパケット送信手段13と、から構成される複数のウィルスチェック装置10a～10nと、ビットにもとづいて、感染パケットPaを検出する感染パケット検出手段21と、感染パケットPaに対応するファイルを実行不可にするファイル実行制御手段22と、から構成されるクライアント端末20a～20mと、ウィルスパターン情報をマルチキャストでウィルスチェック装置10a～10nに配布するウィルスパターン情報配布手段31と、ウィルスパターン情報を一元管理するウィルスパターン情報管理手段32と、から構成されるウィルス情報管理局30と、を有することを特徴とするウィルスチェックネットワーク1が提供される。

【0012】ここで、ウィルスパターン格納手段11は、ウィルスパターンを格納する。ウィルスチェック手段12は、受信したパケットをウィルスパターンにもとづいて、ウィルスに感染している感染パケットPaか否かのウィルスチェックをネットワーク側で行う。パケット送信手段13は、感染パケットPaを検知した場合は、感染を示すパケット内のビットを立てて感染表示パケットPbとして送信する。感染パケット検出手段21は、ビットにもとづいて、感染パケットPaを検出する。ファイル実行制御手段22は、感染パケットに対応するファイルを実行不可にする。ウィルスパターン情報配布手段31は、ウィルスパターン情報をマルチキャストでウィルスチェック装置10a～10nに配布する。ウィルスパターン情報管理手段32は、ウィルスパターン情報を一元管理する。

【0013】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図1は本発明のウィルスチェックネットワークの原理図である。

【0014】ウィルスチェックネットワーク1は、ウィルスチェック装置10a～10nと、クライアント端末20a～20mと、ウィルス情報管理局30と、から構成され、ウィルスチェックを行って、ウィルス侵入を防止する。

【0015】ウィルスパターン格納手段11は、ウィルスパターンを格納する。ウィルスチェック手段12は、受信したパケットと、格納してあるウィルスパターンと、を比較し、パケットがウィルスに感染している感染パケットPaか否かのウィルスチェックをネットワーク側で行う。

【0016】パケット送信手段13は、感染パケットPaを検知した場合は、感染パケットPa内のあらかじめ設定した感染を示すビットを立てて、感染表示パケットPbとして送信する。

【0017】感染パケット検出手段21は、感染表示パケットPbのビットにもとづいて、それが感染パケット

P aと検出する。ファイル実行制御手段 22 は、感染パケット P a に対応するファイルを実行不可にする。

【0018】ウイルスパターン情報配布手段 31 は、最新のウイルスパターン情報をマルチキャストでウイルスチェック装置 10 a ~ 10 n に配布する。配布されたウイルスパターンは、ウイルスパターン格納手段 11 で格納される。

【0019】ウイルスパターン情報管理手段 32 は、ウイルスパターン情報の新規設定、更新等の管理を一元的に行う。次に本発明のウイルスチェックネットワーク 1 を、ルータで構成されているインターネット上のネットワークに適用した場合の実施の形態について以降説明する。本発明のウイルスチェック装置 10 a ~ 10 n をいくつかのルータに配置させ、ネットワーク側でウイルスチェックを行う。

【0020】なお、ウイルスチェック装置を配置したルータを以降では、ウイルスチェックルータと呼ぶ。図 2 はウイルスチェックルータを配置したネットワークの概要を示す図である。ネットワーク 1 は、ルータ R 1 ~ R 8 と、クライアント端末 20 a ~ 20 m と、ウイルス情報管理局 30 と、から構成される。

【0021】図ではルータ R 1、R 2、R 3、R 4 がウイルスチェックルータであり、その他は通常のルータ機能のみを持つ。ウイルスチェックルータ R 2 にウイルス情報管理局 30 が接続し、ウイルスチェックルータ R 4 にクライアント端末 20 a ~ 20 m が接続する。

【0022】ウイルスチェックルータ R 1 ~ R 4 はウイルスのどの部分（先頭部、中間部、終端部）をチェックをするかを分担させており、各担当を最低 1 回は通過するように配置させる。

【0023】各ウイルスチェックルータ R 1 ~ R 4 は、ウイルス情報管理局 30 からマルチキャストで配布されるウイルスパターン V P を受け取り、常に最新のウイルス情報を保持させておく。

【0024】受信したパケットに対し、ウイルスチェックルータ R 1 ~ R 4 は保持してあるウイルスパターン V P と比較する。もし感染している場合にはパケットにビットを立てる。

【0025】その際同時に送信元に対しては警告パケット P w 1 を返し、各ウイルスチェックルータ R 1 ~ R 4 に対しては、警戒情報パケット P w 2 をマルチキャストで配布する。

【0026】警戒情報パケット P w 2 を受け取った各ウイルスチェックルータ R 1 ~ R 4 は、そのウイルスを優先的に検出、あるいは感染元との通信の遮断を行う。クライアント端末 20 a ~ 20 m では、パケットを常に監視しており、感染を示すビットが立っている場合、あるいは警告パケット P w 1 だった場合にはユーザにメッセージを表示し、受け取ったファイルの削除を促す。

【0027】次にウイルスパターン V P について説明す

る。ウイルスパターン V P は、マルチキャストにのせて定期的に配布される。また新種のウイルスが発見されたら、ウイルス情報管理局 30 は新たに作成したウイルスパターン V P をマルチキャストで各ウイルスチェックルータ 10 a ~ 10 n に送り、各ウイルスチェックルータ 10 a ~ 10 n は変更があればウイルスパターンを更新する。

【0028】図 3 はウイルスパターン V P のフォーマットを示す図である。ウイルスパターン V P は、ヘッダ V P - 1 に Ether Hedder と IP Hedder (Multicast) とを持つ。そして、ウイルスパターン配布を示すコード V P - 2 と、ウイルスの種類を示すシリアル番号 V P - 3 と、そのバージョン（改版番号） V P - 4 を持つ。

【0029】これらのあとに、実際のウイルスのバイナリから先頭部分（第 1 領域のウイルスパターン） V P - 6、中間部分（第 2 領域のウイルスパターン） V P - 7、終端部分（第 3 領域のウイルスパターン） V P - 7 を固定長バイトごと抽出したものをつける。

【0030】なお、抽出部分はウイルス情報管理局 30 によって任意に決められ、定期的に変更してバージョン V P - 4 を更新する。また、ウイルスの危険度に応じて脅威レベル V P - 5 をウイルス情報管理局側 30 で決定しておく。これにより危険度に応じた対応を可能にする。

【0031】ウイルスチェックルータ 10 a ~ 10 n では、受け取ったデータを元に自分の持つウイルスパターン V P を後述の検索テーブルに追加する。その際、各ウイルスチェックルータ 10 a ~ 10 n はどの領域を分担するか決められており、受信したパケットから自分の担当するパターンのみを受け取る。

【0032】次にウイルスパターン V P の格納形式について説明する。図 4 はウイルスパターン格納手段 11 の格納形式を示す図である。ウイルスパターン格納手段 11 は、ウイルスパターン V P を検索テーブル 11 a と、シリアル番号保持情報 11 b と、に分けて格納する。

【0033】検索テーブル 11 a は、階層木構造をとる。それぞれ木の深さに応じて第 1 次階層、第 2 次階層、第 3 次階層…と呼ぶ。また、それぞれの枝部分とシリアル番号を対応させておく。

【0034】シリアル番号保持情報 11 b は、現在自分の持っているシリアル番号とバージョンと脅威レベルを保持しており、ウイルスパターン V P のマルチキャストパケットが来た際、これと比較して変更が必要かどうかを判断する。

【0035】次に検索テーブル 11 a に新規にウイルスパケット V P を追加する場合の処理について説明する。各ウイルスチェックルータ 10 a ~ 10 n は、自分の保持しているウイルスパターン V P のシリアル番号と、バージョン番号と、をシリアル番号保持情報 11 b に検索テーブル 11 a とは別に保管している。

【0036】マルチキャストによる新規のウィルスパターンVPから自分の担当分を受け取ると、ウィルスパターンVP情報を記録したシリアル番号保持情報11bをもとにウィルスパターンVPの検索テーブル11aを更新する。

【0037】まず、シリアル番号とバージョンをチェックして変更が必要か判断する。変更が必要と判断すると検索テーブル11aの第1次階層、第2次階層、…と比較していつて重ならなくなる部分を探し、そこから新規に枝を伸ばす。その後、新規追加した枝を最上位に移動させ、登録を終了する。

【0038】図5はウィルスパターン格納手段11でのウィルスパターンVPを新規登録する際の処理手順を示すフローチャートである。

〔S1〕シリアル番号を自分のウィルスチェックルータ内に持っているかどうかを判断する。持っている場合はステップS2へ、持っていない場合はステップS4へ行く。

〔S2〕バージョン更新かどうかを判断する。更新ならばステップS3へ、更新でなければ終了する。

〔S3〕対象のシリアル番号の枝を削除する。

〔S4〕第1次階層と比較する。ステップS4の詳細は図6で説明する。

【0039】図6は第n次階層と比較して、新たに枝を作成する際の処理手順を示すフローチャートである。

〔S10〕ウィルスパターンから1文字とる。

〔S11〕既存の検索テーブル11aの第n次階層と比較する。

〔S12〕ヒットした場合はステップS13へ、そうでなければステップS14へ行く。

〔S13〕次の第n+1次階層と比較する。

〔S14〕枝を追加する。

〔S15〕枝の優先順位を上にもってくる。

【0040】以上説明したような処理手順で、新種のウィルスパターンVPに対して対応する枝を作成していき格納しておく。次にウィルスチェックルータ10の構成について説明する。図7はウィルスチェックルータ10の構成を示す図である。

【0041】図に示す通常の packets は、本発明のウィルスチェック手段12に該当するウィルスチェックフィルタ12でウィルスチェックが行われる。ここでウィルスチェックを行うべき packets は、packets の中身がTCPかつftp、http、smtpのいずれかの packets で、かつまだチェックが完了していない packets である。

【0042】ただし、それ以外の packets は、負荷軽減のためウィルスチェックフィルタ12をウィルスチェックせずに通過させる。また、オフセット値がある一定以上の packets、つまりフローの後ろの方の packets も通過させる。なお、この際ウィルスチェック済みの packets

を立てる。

【0043】一方、マルチキャストの packets は、シリアル番号保持情報11bでウィルスパターンの更新処理が行われ、検索テーブル11aに階層木構造形式で格納される。

【0044】そして、経路計算部13aで経路計算をした後、packets 生成送信部13bは、ウィルスチェックに引っかかった packets に対して、後述のIPヘッダのオプションのフィールドにビットを立てた感染表示 packets Pbを生成する。以降の同一のフローの packets に対してもビットを立てる。

【0045】また、packets 生成送信部13bは、IP packets の送信元に向けて警告 packets Pw1を生成する。その後、感染表示 packets Pb、警告 packets Pw1を送信する。

【0046】なお、警戒モードに設定して、感染元との通信を遮断する警戒モード設定手段14については後述する。一方、クライアント端末20では、ソフトウェアによってIPヘッダのウィルス感染を示すビットを監視している。ビットが立った感染表示 packets Pb及び警告 packets Pw1を受け取ったクライアント端末20は、ユーザに対してウィルスに感染した旨のメッセージ表示を行う。

【0047】次にIPヘッダの構成について説明する。図8はIPヘッダの構成を示す図である。バージョンは4ビットで、インターネットヘッダの形式を示す。IH L (Internet Header Length) は4ビットで、ヘッダ長が32ビットワード単位で示される。サービスタイプは8ビットで、スループット等のサービス品質が示される。全長は16ビットで、オクテット単位で図った長さを示す。なお、全長にはヘッダとデータとを含む。

【0048】識別番号は16ビットで、送信側を識別するために割り当てられた値でデータグラムのフラグメントを組み立てる際に使用される。Flagは3ビットで、フラグメントの分割許可または継続等の制御を示す。フラグメントオフセットは13ビットで、データグラム内でフラグメントの占める位置を示す。

【0049】ttlは8ビットでデータグラムがインターネットのシステムに留まっていられる時間の最小値を示す。プロトコルは8ビットで、データグラムのデータ部を渡すべきトランスポートレイヤプロトコルを示す。ヘッダチェックサムは16ビットでヘッダに対するチェックサムを示す。

【0050】始点アドレスは32ビットで、始点のIPアドレスを示す。終点アドレスは32ビットで終点のIPアドレスを示す。オプションは可変長で、ユーザが任意に定義できる。本発明ではこのオプション領域を利用して感染表示 packets Pb、警告 packets Pw1及び警戒情報 packets Pw2を生成する。

【0051】次にウィルスチェック手段12について説

明する。図9はウィルスチェックの処理手順を示すフローチャートである。

〔S20〕すでに別のウィルスチェックルータでチェック済みかどうかを判断する。チェック済みならステップS30へ、そうでない場合はステップS21へ行く。

〔S21〕オフセット値が一定以上かどうかを判断する。一定以上の場合はステップS30へ、そうでなければステップS22へ行く。

〔S22〕TCPパケットでかつhttp、ftp、smtpのいずれかのパケットかどうかを判断する。その場合はステップS23へ、そうでなければステップS30へ行く。

〔S23〕ウィルスチェックを行う。なお、詳細は図10で説明する。

〔S24〕感染しているかどうかを判断する。感染している場合はステップS28へ、そうでなければステップS25へ行く。

〔S25〕次のパケットの1バイトをとる。

〔S26〕終了かどうかを判断する。終了の場合はステップS27へ、そうでなければステップS23へ戻る。

〔S27〕チェック済みのビットを立てる。

〔S28〕IPヘッダのオプションフィールドにビットを立てる。

〔S29〕警告パケットPw1、警戒情報パケットPw2を発行する。

〔S30〕経路計算を行う。

【0052】次に上記のステップS23のウィルスチェックルーティンについて説明する。パケット内の1バイトを取り、まず検索テーブル11a内の第1次階層と比較する。同じものがあつた場合は、パケットから次の1バイトを取り、一致した枝の配下の第2次階層と比較する。

【0053】もし当てはまらなくなつたらパケットの次の1バイトを取り出して最初から比較をやり直す。これを繰り返し最後まで当てはまる場合は、このバイトはウィルスに感染したと判断しIPヘッダのオプションのフィールドのビットを立てる。

【0054】また、もし検索の途中でパケットが終了した場合は感染していないものとみなし、代わりに別の領域を担当しているウィルスチェックルータにまかせる。図10はウィルスチェックルーティンの処理手順を示すフローチャートである。

〔S40〕パケットから1バイトを取り出す。

〔S41〕パケット完了かどうかを判断する。パケット完了の場合は終了し、そうでなければステップS42へ行く。

〔S42〕ウィルスパターン第n次階層と比較する。

〔S43〕ヒットしたかどうかを判断する。ヒットした場合はステップS46へ、そうでなければステップS44へ行く。

〔S44〕階層を1次に戻す。

〔S45〕第1次階層をチェックする。

〔S46〕階層をn+1次にする。

〔S47〕ウィルスチェック完了かどうかを判断する。完了の場合はステップS49へ、そうでなければステップS48へ行く。

〔S48〕第n+1次階層をチェックする。

〔S49〕ウィルス感染と判断する。

【0055】次にウィルスチェック時に立てるビットについて説明する。ウィルスチェックルータでウィルスチェックを実施すると、まずIHLフィールドを1増加してオプション領域を確保する。そして、確保されたオプション領域にビットを立てる。

【0056】図11は感染表示パケットPbのIPパケットのフォーマットを示す図である。まず、IHLフィールドを1増加する。そして、オプション領域をThe Copied flag=0、The option Classes=3（将来の予約用領域）、The option Number=1（感染表示パケットPb：ウィルスチェックをしたことを示すコード）、Length=5と設定する。

【0057】また、Option Valueとして第1ビットは第1領域チェック未／済、第2ビットは第2領域チェック未／済、第3ビットは第3領域チェック未／済と割り当てる。すなわち、ウィルスチェックをしたかどうかの情報を記す。

【0058】そして、第4ビットはウィルス未感染／感染を示し、未感染なら0、感染している場合は1を立てて、感染表示パケットPbを表す。なお、第5ビット以降はシリアル番号である。

【0059】次に警告パケットPw1について説明する。ウィルスチェックルータでウィルスを検知した際に送信元には警告パケットPw1を送信し、周囲のウィルスチェックルータには警戒情報パケットPw2をマルチキャストで送信する。これによってウィルスの早期発見、拡大防止をはかる。

【0060】警告パケットPw1は、ウィルス検知時のパケットと同様にIPヘッダのオプション領域のビットを立て、以下のフォーマットで送信元に配送される。図12は警告パケットPw1のフォーマットを示す図である。まず、IHLフィールドを1増加する。そして、オプション領域をThe Copied flag=0、The option Classes=3（将来の予約用領域）、The option Number=2（警告パケットPw1を示すコード）、Length=3と設定する。そして、図11で説明したチェック未／済のオプションを付加する。また、終点アドレスが感染元のアドレスとなる。

【0061】次にクライアント側の処理について説明する。図13はクライアント端末20の構成を示す図である。本発明の感染パケット検出手段21はLANドライバ21aに、ファイル実行制御手段22はTCP/IP

ドライバ22bに含まれる。

【0062】LANドライバ21aは、送られてくる各フローについて、各パケットのウィルスチェックビットを見る。そして、ビットが立っているかどうかを判断し、その結果をTCP/IPドライバ22bに通知する。

【0063】TCP/IPドライバ22bは、ビットが立っている旨の通知を受けると、対応するファイルを実行不可にした後、ファイルを削除する旨のメッセージ20-1を表示する。

【0064】次にクライアント端末20でのビット監視の流れについて説明する。図14、図15はクライアント端末20のビット監視の処理手順を示すフローチャートである。

〔S50〕パケットを読み込む。

〔S51〕新規のフローかどうかを判断する。新規のフローの場合はステップS52へ、そうでなければステップS53へ行く。

〔S52〕フロー情報を追加する。

〔S53〕終了フローかどうかを判断する。終了フローの場合はステップS54へ、そうでなければステップS55へ行く。

〔S54〕フロー情報から該当フローを削除する。

〔S55〕ビットをチェックする。

〔S56〕ヒットしたかどうかを判断する。ヒットした場合はステップS58へ、そうでなければステップS57へ行く。

〔S57〕TCP/IPドライバ22bに処理を渡す。

〔S58〕警告パケットPw1かどうかを判断する。警告パケットの場合はステップS59へ、そうでなければステップS60へ行く。

〔S59〕警告の旨のメッセージを表示する。

〔S60〕ファイルの実行権をなくす。

〔S61〕警告メッセージ20-1の表示を行う。

【0065】次に警戒情報パケットPw2について説明する。ウィルスチェックルータでウィルス検知された際、各ウィルスチェックルータにはマルチキャストで警戒情報パケットPw2を出す。警戒情報パケットPw2はウィルスパケットのシリアル番号と送信元IPアドレスを情報として持ち、マルチキャストで配布される。

【0066】警戒情報パケットPw2を受け取った各ウィルスチェックルータは受け取ったシリアル番号のウィルスパターンVPの検索の優先順位を上げる。図16は警戒情報パケットPw2のフォーマットを示す図である。警戒情報パケットPw2は、ヘッダPw2-1にEther HedderとIP Hedder(Multicast)を持つ。

【0067】そして、警戒情報を示すコードPw2-2と、ウィルスの種類を示すシリアル番号Pw2-3と、そのバージョン(改版番号)Pw2-4を持つ。さらに、ウィルスの危険度に応じた脅威レベルPw2-5

と、ウィルス感染元のIPアドレスPw2-6をつける。

【0068】次に警戒情報パケットPw2を受け取った際の検索順番の処理手順について説明する。図17は警戒情報パケットPw2を受け取った際の検索順番の処理手順を示す図である。

〔S70〕警戒情報パケットPw2からシリアル番号を取得する。

〔S71〕第1次階層、第2次階層、…第n次階層、の検索順位を最上位に上げる。

【0069】次に感染元との通信遮断を行うための警戒モード設定手段14について説明する。脅威レベルがある一定以上の場合、拡大を防止するためウィルスチェックルータ側でホストとの通信を一定時間遮断させる。

【0070】警戒情報パケットPw2の中の脅威レベルを見て、ある一定以上の場合にはIPアドレスをテーブルに保存し、警戒モードに移行する。警戒モードでは通常の処理の前にくるパケットをチェックし、テーブルにあるアドレスから来たパケットと、テーブルにあるアドレスに向かうパケットと、を一定時間だけすべて廃棄する。

【0071】廃棄させる時間は、再送要求がタイムアウトする程度の時間とし、テーブルに保存された時にカウンタと一緒に設定される。もしこの時間内にパケットが来なかったらテーブルから削除し、警戒モードを解除する。逆にパケットが来たら時間(カウンタのカウント値)を延長させる。

【0072】図18は警戒モード設定手段14が行う警戒モードの処理手順を示すフローチャートである。

〔S80〕脅威レベルは一定以上かどうかを判断する。一定以上の場合、ステップS81へ、そうでなければステップS89へ行く。

〔S81〕警戒IPアドレスを保持する警戒IPアドレステーブルにIPアドレスと、警戒モードにしておく時間をカウントするカウンタ値と、を設定する。

〔S82〕パケットを読み込む。

〔S83〕始点/終点のアドレスがテーブルと一致するかどうかを判断する。一致する場合はステップS84へ、そうでなければステップS86へ行く。

〔S84〕パケットを廃棄する。

〔S85〕カウンタ値を延長する。すなわち、警戒モードにする時間をさらに長くする。

〔S86〕カウンタ値を減少する。すなわち、警戒モードにする時間を短くする。

〔S87〕カウンタを終了するかどうかを判断する。終了の場合はステップS88へ、終了しない場合はステップS82へ戻る。

〔S88〕警戒IPアドレステーブルからIPアドレスと、カウンタ値を削除する。

〔S89〕通常モードにする。

【0073】次にウイルスチェックルータの協調による負荷分散及びチェック精度向上について説明する。ウイルスのバイナリデータは小さく、パケットをまたがってバイナリが分割してしまう場合がある。したがって、各ウイルスチェックルータ毎に担当するウイルスパターンVPを異なるように分担させ保持させる。

【0074】これにより、もしある領域で仮りにパケットの途中でウイルスのバイナリが切れてしまった場合でも、別なパケットでは別の領域のチェックにかかるようになる。

【0075】ウイルスチェックルータに対するウイルスパターンの各分担は、手動でも自動でも設定可能とする。ただし、手動で設定する場合は、パケットは受信先に到着するまでにはすべての領域がチェックされるような構成、つまりそれぞれ分担しているウイルスチェックルータを最低1回ずつは通るような構成にする必要がある。

【0076】次に自動で設定する場合について説明する。図19は担当分担領域要求パケットのフォーマットを示す図である。図に示すフォーマットを用いて自動設定する。

【0077】まず、新規のウイルスチェックルータは担当分担領域要求パケット100を自分が配布可能な全てのウイルスチェックルータに配布する。この場合ttl領域は小さく設定して、余計な負荷は極力かけないようにしておく必要がある。

【0078】また、自分が持つルーティング情報から自分の接続している全ウイルスチェックルータそれぞれに対して、終点アドレスを挿入したパケットを発行する。オプション領域は、The Copied flag=0、The option Classes=3（将来の予約用領域）、The option Number=3（担当分担領域要求パケット100を示すコード）、Length=3、「空き」と設定する。

【0079】この担当分担領域要求パケット100を受け取った各ウイルスチェックルータは、送信元に対して自分の担当領域を以下のような担当領域要求応答パケット101にのせて返送する。図20は担当分担領域要求応答パケット101のフォーマットを示す図である。

【0080】ttlがまだ残っていれば、自分が受け取ったウイルスチェックルータ以外の配送できる範囲の全てのウイルスチェックルータに対して同報する。担当分担領域要求応答パケット101のオプション領域は、The Copied flag=0、The option Classes=3（将来の予約用領域）、The option Number=4（担当分担領域要求応答パケット101を示すコード）、Length=3、「担当領域」と設定する。

【0081】また、送信側のウイルスチェックルータは、返ってきた担当分担領域要求応答パケット101から各領域を担当しているルータの台数を集計して、最も担当しているルータの少ない領域を自分の担当領域とす

る。

【0082】以上説明したように、本発明のウイルスチェックネットワーク1は、ウイルスチェックルータにウイルスチェック機能を搭載させることにより、ネットワーク側でウイルスを検知させることができ、ウイルス侵入防止をより多くのクライアントに対して、またより確実に行うことができる。

【0083】また、常に最新のウイルスパターン情報をウイルスチェックルータ間でマルチキャストにより交換通知し、またその更新方法もマルチキャストのパケットを発行するだけであるので、新たなウイルスへの対応が簡単にかつ迅速に行うことができる。またクライアント側で更新をかける必要がない。

【0084】さらに、検知したウイルスに対する警告を各ウイルスチェックルータが同時に行うことで早期発見、拡大防止を図る。そして、送信元に対しても警告パケットを送ることでウイルス感染を通知することができる。

【0085】また、各ウイルスチェックルータでウイルスチェック領域を分担することで、各々ウイルスチェックルータにかかる負荷を分散することができ、フレーム間にまたがってウイルスが存在する場合においてもいずれかを担当しているウイルスチェックルータでチェックすることができ、ウイルスチェックの精度が向上する。

【0086】さらに、ウイルスが検知されたパケットを落とすことはせずに、IPヘッダにビットを立てて受信側に通知することで再送などによる余計なトラフィックの増加を防ぐことができる。そして、ウイルスの脅威レベルに応じて通信を遮断させるため、感染の拡大を防止させることができる。

【0087】

【発明の効果】以上説明したように、本発明のウイルスチェックネットワークは、複数のウイルスチェック装置を設けて、ネットワーク側でウイルスチェックを行う構成とした。これにより、ネットワーク側でウイルスを未然に防ぐことができるので、ウイルスの感染及び拡大を防止でき、ウイルスチェック対策効率の向上を図ることが可能になる。

【図面の簡単な説明】

【図1】本発明のウイルスチェックネットワークの原理図である。

【図2】ウイルスチェックルータを配置したネットワークの概要を示す図である。

【図3】ウイルスパターンVPのフォーマットを示す図である。

【図4】ウイルスパターンVP格納手段の格納形式を示す図である。

【図5】ウイルスパターン格納手段でのウイルスパターンVPを新規登録する際の処理手順を示すフローチャートである。

15

【図6】第n次階層と比較して、新たに枝を作成する際の処理手順を示すフローチャートである。

【図7】ウイルスチェックルータの構成を示す図である。

【図8】IPヘッダの構成を示す図である。

【図9】ウイルスチェックの処理手順を示すフローチャートである。

【図10】ウイルスチェックルーティンの処理手順を示すフローチャートである。

【図11】感染表示パケットのIPパケットのフォーマットを示す図である。

【図12】警告パケットのフォーマットを示す図である。

【図13】クライアント端末の構成を示す図である。

【図14】クライアント端末のビット監視の処理手順を示すフローチャートである。

【図15】クライアント端末のビット監視の処理手順を示すフローチャートである。

【図16】警戒情報パケットのフォーマットを示す図である。

【図17】警戒情報パケットを受け取った際の検索順番

16

の処理手順を示す図である。

【図18】警戒モードの処理手順を示すフローチャートである。

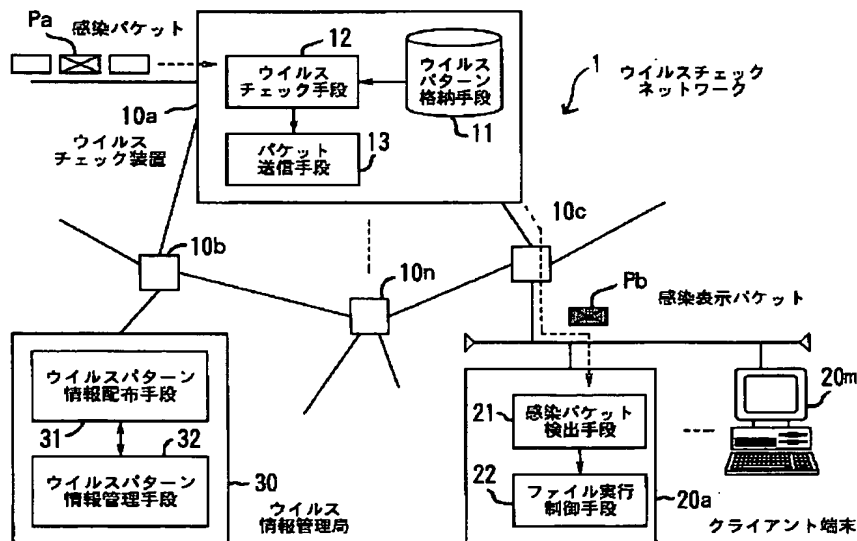
【図19】担当分担領域要求パケットのフォーマットを示す図である。

【図20】担当分担領域要求応答パケットのフォーマットを示す図である。

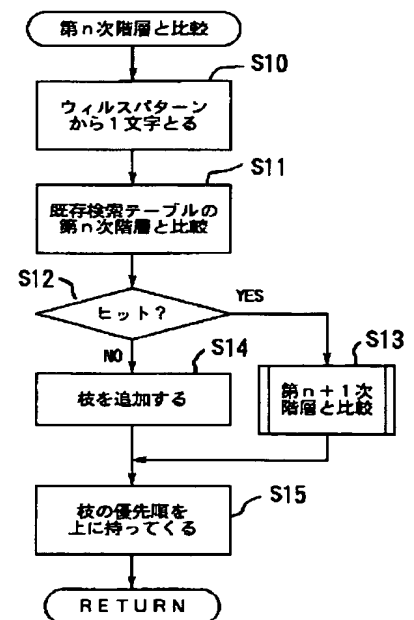
【符号の説明】

- 1 ウイルスチェックネットワーク
- 10a～10n ウイルスチェック装置
- 11 ウイルスパターン格納手段
- 12 ウイルスチェック手段
- 13 パケット送信手段
- 20a～20m クライアント端末
- 21 感染パケット検出手段
- 22 ファイル実行制御手段
- 30 ウイルス情報管理局
- 31 ウイルスパターン情報配布手段
- 32 ウイルスパターン情報管理手段
- 20 Pa 感染パケット
- Pb 感染表示パケット

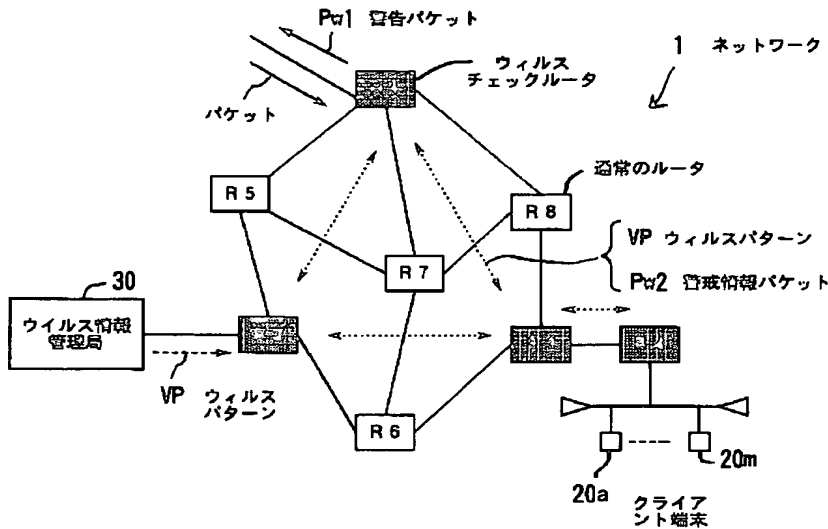
【図1】



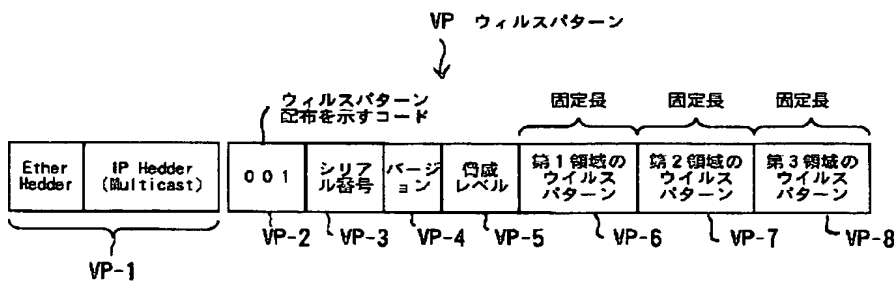
【図6】



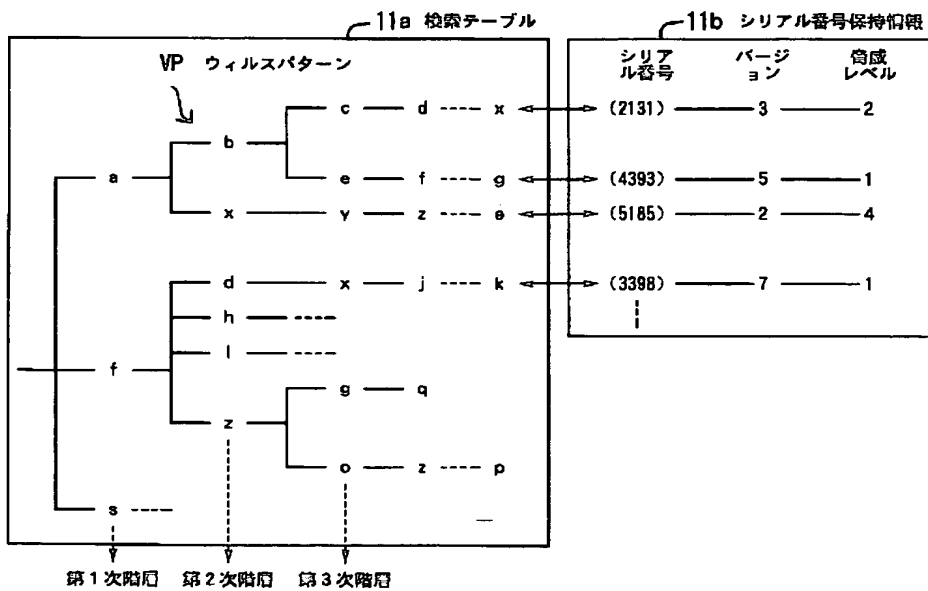
【図2】



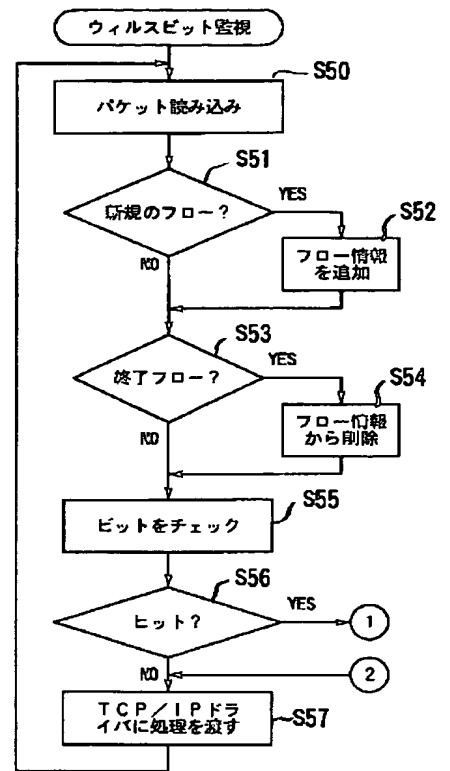
【図3】



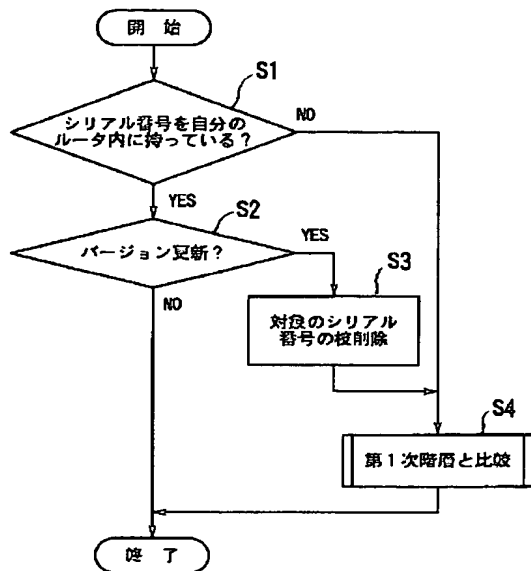
【図4】



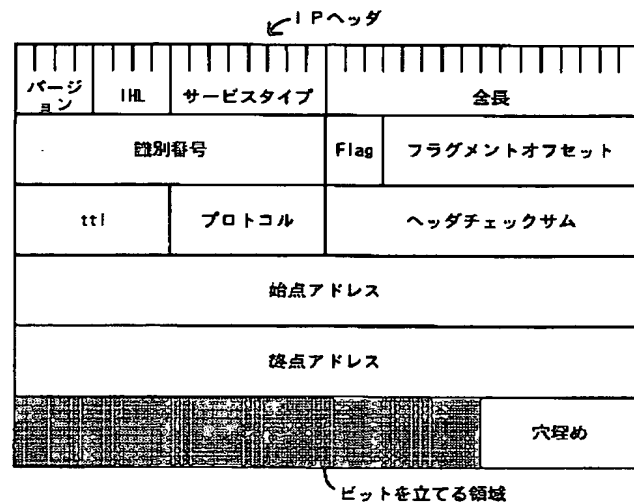
【図14】



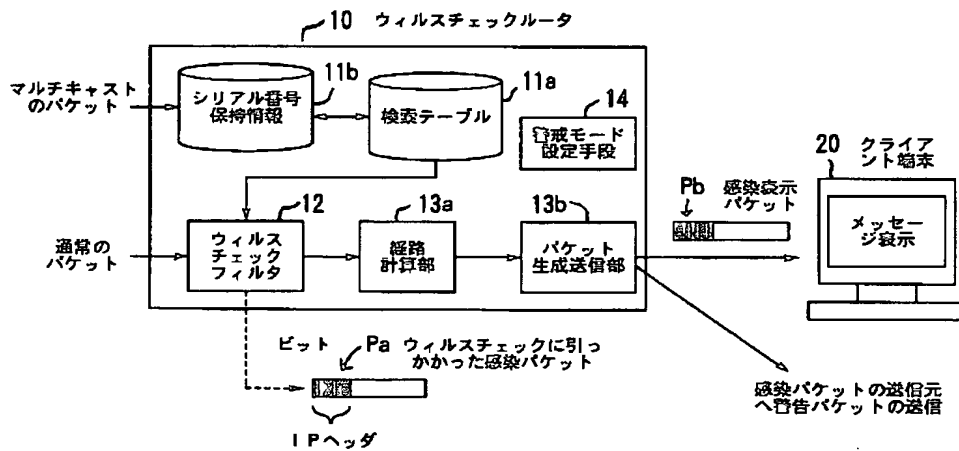
【図5】



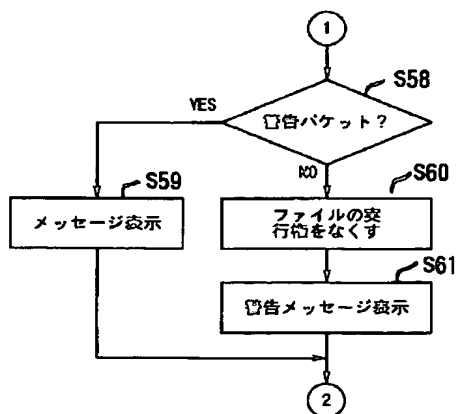
【図8】



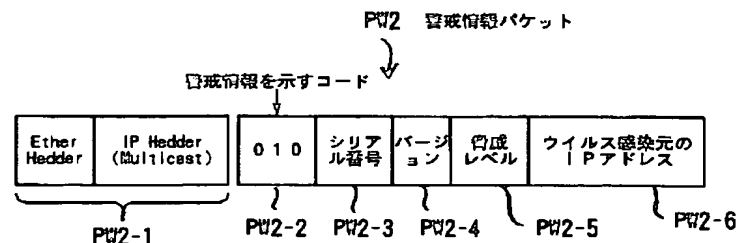
【図7】



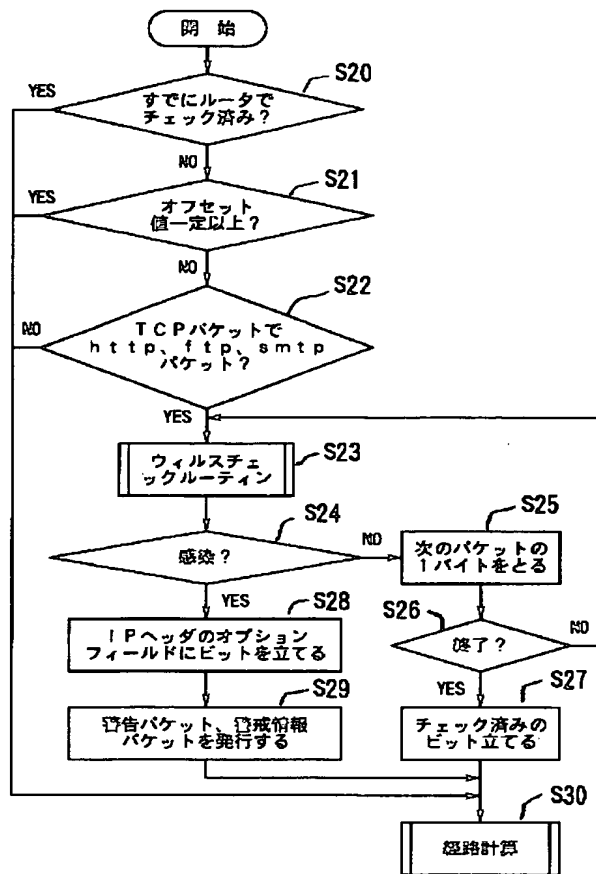
【図15】



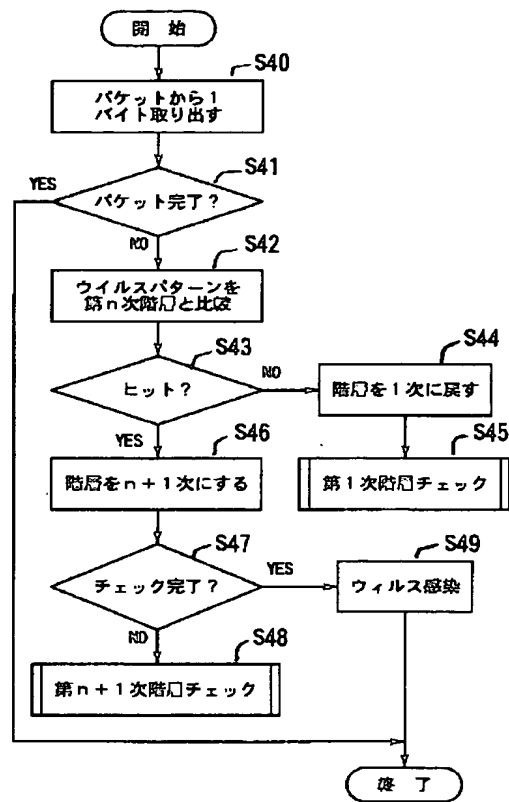
【図16】



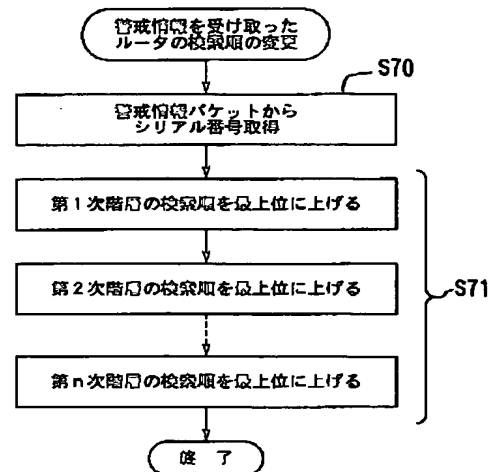
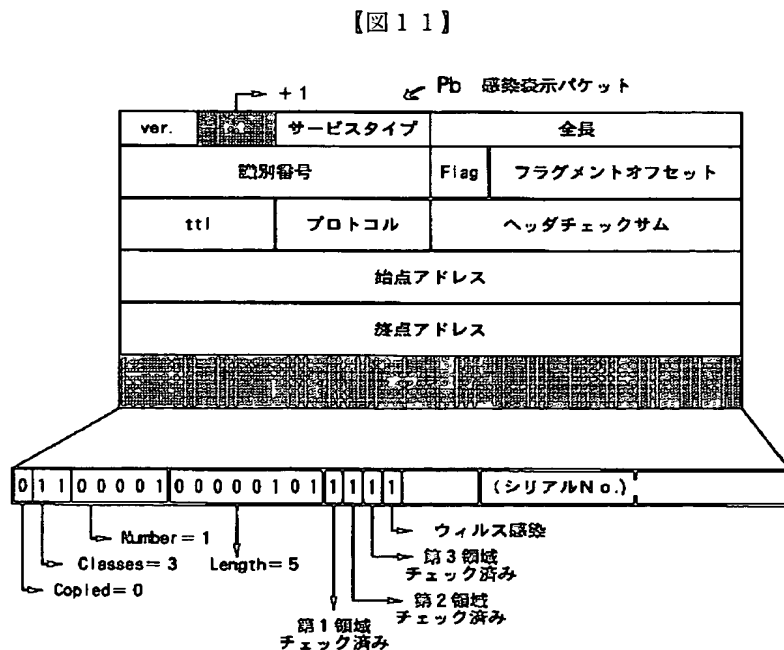
【図9】



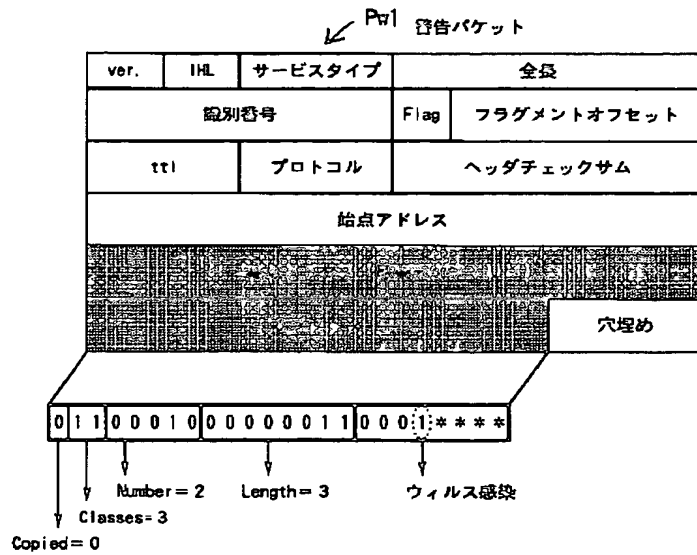
【図10】



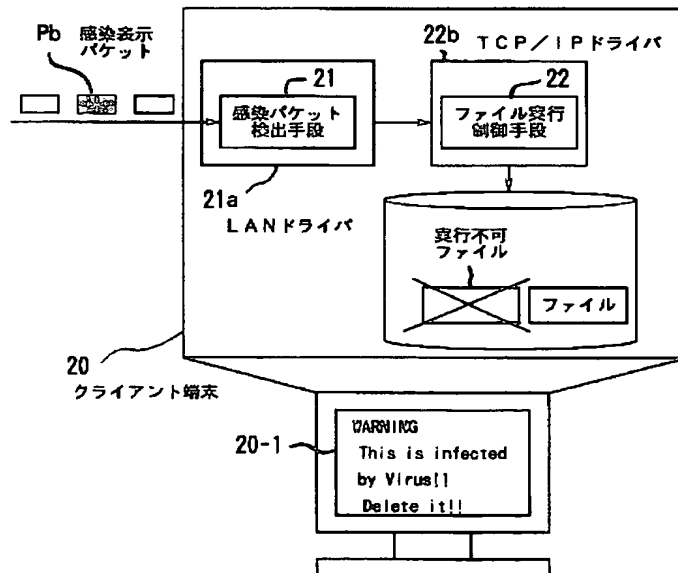
【図17】



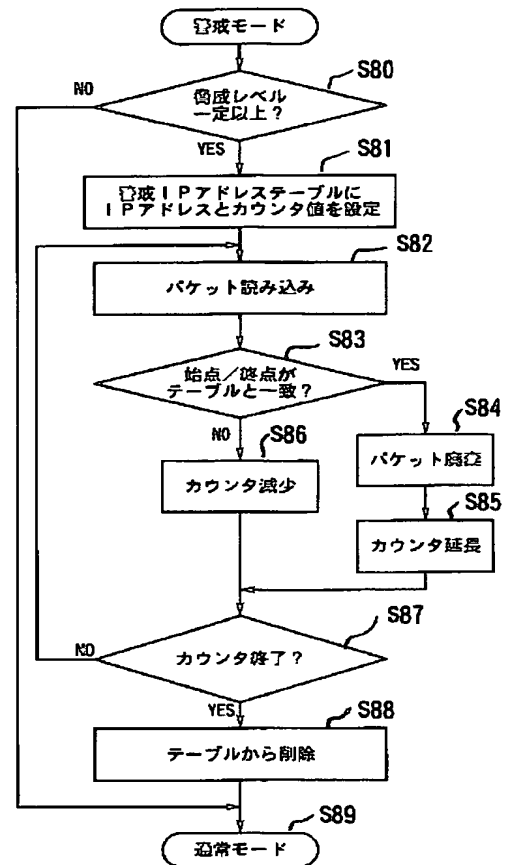
【図12】



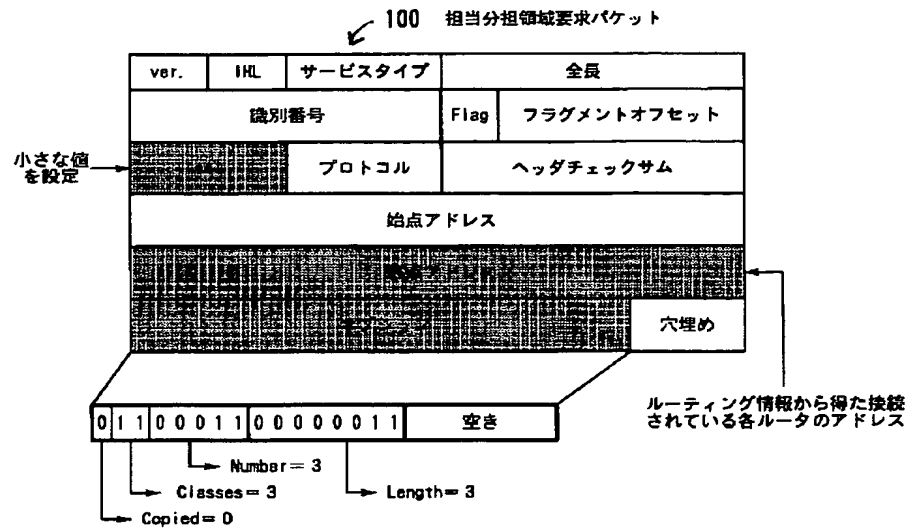
【図13】



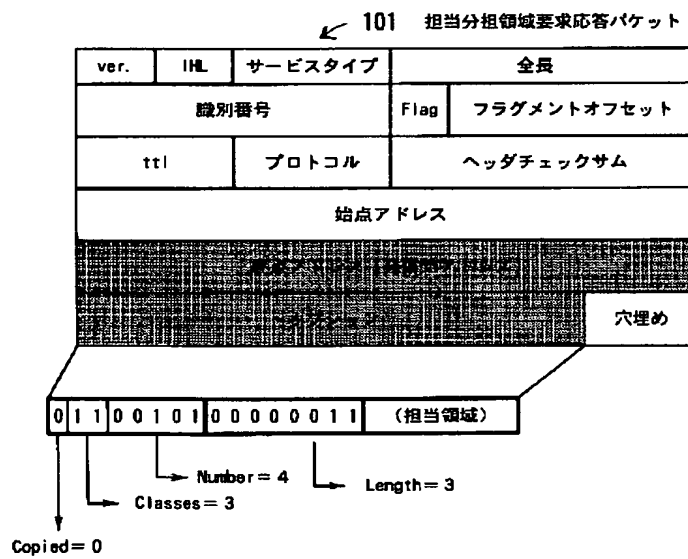
【図18】



【図19】



【図20】



11-167487

[0013]

[Embodiments] An embodiment of the present invention will be described with reference to the drawings below. Fig. 1 shows the principles of a virus check network in accordance with the present invention.

[0014] A virus check network 1 comprises virus checking devices 10a to 10n, client terminals 20a to 20m, and a virus information management station 30, and it checks for a virus so as to prevent infection by the virus.

[0015] Virus patterns are stored in a virus pattern storage means 11. A virus checking means 12 compares a received packet with the stored virus patterns, and thus performs a virus check on a network side so as to check if a received packet is a packet Pa infected with a virus.

[0016] If an infected packet Pa is detected, a packet transmitting means 13 sets a predetermined bit contained in the infected packet Pa so as to indicate infection, and transmits the packet as an infection-indicated packet Pb.

[0017] Based on the bit in the infection-indicated packet Pb, an infected packet detecting means 21 recognizes the packet as the infected packet Pa. A file execution control means 22 disables execution of a file corresponding to the infected packet Pa.

[0018] A virus pattern information distributing means 31 multicasts the latest virus pattern information to the virus checking devices 10a to 10n. The distributed virus pattern is stored in the virus pattern storage means 11.

[0019] A virus pattern information managing means 32 performs all management jobs including determination of virus pattern information and the updating thereof. Next, a description will be made of a case where the embodiment of the virus check network 1 of the present invention is adapted to a network on the Internet which comprises routers. The virus checking devices 10a to 10n employed according to the present invention are allocated to some routers in order to check for a virus on the network side.

[0020] Incidentally, the routers to which the virus checking devices are allocated shall be called virus checking routers. Fig. 2 schematically shows a network accommodating the virus checking routers. The network 1 comprises routers R1 to R8, the client terminals 20a to 20m, and the virus information management station 30.

[0021] In the drawing, the routers R1, R2, R3, and R4 are the virus checking routers, and the other routers have only the capabilities of a normal router. The virus information management station 30 is connected to the virus checking router R2, and the client terminals 20a to 20m are connected to the virus checking router R4.

[0022] The virus checking routers R1 to R4 are assigned to jobs of checking for respective parts of a virus (leading part, intermediate part, and trailing part). The virus checking routers R1 to R4 are arranged so that a packet will pass through the routers at least once.

[0023] Each of the virus checking routers R1 to R4 receives a virus pattern VP multicast from the virus information management station 30, and holds the latest virus information all the time.

[0024] Each of the virus checking routers R1 to R4 compares a received packet with the held virus pattern VP. If a received packet is infected with a virus, a bit in the packet is set.

[0025] At the same time, a warning packet Pw1 is returned to a transmitting source, and a caution information packet Pw2 is multicast to the virus checking routers R1 to R4.

[0026] Each of the virus checking routers R1 to R4 having received the caution information packet Pw2 detects the virus concerned as a top priority or discontinues communication with an infecting source. The client terminals 20a to 20m always monitor a packet. If a bit indicating infection is set or if a received packet is the warning packet Pw1, a message is displayed in order to prompt a user to delete the received file.

[0040] According to the foregoing procedure, a branch in a hierachical tree structure is created corresponding to each new kind of virus pattern VP, and then stored. Next, the configuration of the virus checking router 10 will be described. Fig. 7 shows the configuration of the virus checking router 10.

[0041] As illustrated, a normal packet is checked for a virus by a virus checking filter 12 corresponding to the virus checking means 12 employed in the present invention. Herein, a packet that should be checked for a virus is any packet which specifies TCP and ftp, http, or smtp and whose check has not been completed.

[0042] However, the other packets are passed through the virus checking filter 12 without being checked for a virus in efforts to lighten the load on the virus checking filter. A packet provided with an offset value equal to or larger than a certain value, that is, a packet to be transmitted late in a data flow is also passed. At this time, a bit indicating that a virus check has been completed is set.

[0043] On the other hand, a virus pattern specified in the serial number hold information 11b is updated with a virus pattern specified in a multicast packet. The virus pattern specified in the multicast packet is stored in the search table 11a according to a hierarchical tree structure.

[0044] After a route calculator 13a calculates a route, a packet production and transmission block 13b produces the infection-indicated packet Pb by setting the bits in an option field of an IP header of a packet that is recognized to be infected with a virus during a virus check. The bits are set in subsequent packets to be transmitted within the same data flow.

[0045] Moreover, the packet production and transmission block 13b produces a warning packet Pw1 that is duly transmitted to a transmitting source from which the IP packet has been transmitted. Thereafter, the infection-indicated packet Pb and warning packet Pw1 are transmitted.

[0046] A caution mode designating means 14 that designates a

caution mode, so as to discontinue communication with an infecting source, will be described later. On the other hand, the client terminals 20 use software to monitor a bit that is contained in an IP header in order to indicate infection with a virus. Any of the client terminals 20 having received the infection-indicated packet Pb that has the bit set and the warning packet Pw1 displays for a user a message saying that a packet has been infected with a virus. [0047] Next, the structure of an IP header will be described. Fig. 8 shows the structure of an IP header. A version field is four bits long and specifies the format of an Internet header. An Internet header length (IHL) field is four bits long and specifies a header length in 32-bit words. A service type field is eight bits long and specifies service quality such as a throughput. An overall length field is sixteen bits long and specifies a length measured in octets. Incidentally, the overall length includes the lengths of the header and data.

[0048] An identification number field is sixteen bits long and specifies a value which is assigned to a transmitting side so that the transmitting side can be identified with the value and which is used to assemble fragments of a datagram. A flag field is three bits long and specifies that division of a fragment is enabled or continued or that control is extended in a certain manner. A fragment offset field is thirteen bits long and specifies a position in a datagram occupied by a fragment.

[0049] A time to live (ttl) field is eight bits long and specifies the minimum value of a time during which a datagram can stay in an Internet system. A protocol field is eight bits long and specifies a transport layer protocol according to which data in a datagram should be handed. A header checksum field is sixteen bits long and specifies a checksum to be adopted for a header.

[0050] A start address field is 32 bits long and specifies an IP address of a start point. An end address field is 32 bits long and specifies an IP address of an end point. An

option field has a variable length and can be defined arbitrarily by a user. According to the present invention, the option field is used to produce the infection-indicated packet Pb, warning packet Pw1, and caution information packet Pw2.

[0051] Next, the virus checking means 12 will be described. Fig. 9 is a flowchart describing a virus check procedure.

S20: It is judged whether any other virus checking router has checked a packet. If any other virus checking router has checked a packet, control is passed to step S30. Otherwise, control is passed to step S21.

S21: It is judged whether an offset value is equal to or larger than a certain value. If an offset value is equal to or larger than a certain value, control is passed to step S30. Otherwise, control is passed to step S22.

S22: It is judged whether the packet is conformable to the TCP and any of the http, ftp, and smtp. If so, control is passed to step S23. If not, control is passed to step S30.

S23: A virus check is performed. The details will be described in conjunction with Fig. 10.

S24: It is judged whether the packet is infected with a virus. If the packet is infected with a virus, control is passed to step S28. Otherwise, control is passed to step S25.

S25: One byte of the next packet is sampled.

S26: It is judged whether the byte is the last byte of the packet. If the byte is the last byte, control is passed to step S27. Otherwise, control is returned to step S23.

S27: A bit indicating that a virus check has been completed is set.

S28: The bits in the option field of an IP header are set.

S29: The warning packet Pw1 and caution information packet Pw2 are issued.

S30: A route is calculated.

[0052] Next, the virus check routine to be executed at step

S23 above will be described. One byte of a packet is sampled and compared with the first hierarchical level in the search table 11a. If the same character as the one represented by the one byte is found in the first hierarchical level, the next one byte is sampled from the packet, and compared with the second hierarchical level subordinate to the branch in which the same character as the one represented by the one byte is found.

[0053] If the same character as the one represented by one byte is not found, the next one byte is sampled from the packet and compared with the first hierarchical level again. After the comparison is repeated, if the same character as the one represented by the last one byte is found, the byte is judged to have been infected with a virus. The bits in the option field of the IP header are set.

[0054] If a packet comes to an end in the course of search, the packet is judged not to have been infected with a virus. The packet is transferred to any other virus checking router responsible for other part of a virus pattern. Fig. 10 is a flowchart describing a procedure of a virus checking routine.

S40: One byte is sampled from a packet.

S41: It is judged whether the one byte is the last one byte. If the one byte is the last one byte, the routine is terminated. Otherwise, control is passed to step S42.

S42: Another part of the packet is compared with a part of the virus pattern specified in the n-th hierarchical level.

S43: It is judged whether the search is a hit. If the search is a hit, control is passed to step S46. Otherwise, control is passed to step S44.

S44: The hierarchical level is returned to the first hierarchical level.

S45: The first hierarchical level is checked.

S46: The hierarchical level is set to the n+1-th hierarchical level.

S47: It is judged whether the virus check is completed. If the virus check is completed, control is passed to step

S49. Otherwise, control is passed to step S48.

S48: The $n+1$ -th hierarchical level is checked.

S49: It is judged that the packet has been infected with a virus.

[0055] Next, bits to be set at the time of a virus check will be described. When a virus checking router performs a virus check, the value specified in the IHL field is incremented by one in order to preserve the option field. The bits in the preserved option field are set.

[0056] Fig. 11 shows the format of an IP packet adopted for the infection-indicated packet Pb. First, the value in the IHL field is incremented by one. The copied flag bit in the optical field is set to 0. The option class bits therein are set to represent 3 (field preserved for the future), the option number bits therein are set to represent 1 (code indicating that the infection-indicated packet Pb has undergone a virus check), and the length bits are set to represent 5.

[0057] Moreover, as an option value, the first bit is assigned to an indication that the first part of a packet has been, or has not been, checked for the first part of a virus pattern. The second bit is assigned to an indicating that the second part of the packet has been, or has not been, checked for the second part of the virus pattern. The third bit is assigned to an indication that the third part of the packet has been, or has not been, checked for the third part of the virus pattern. Namely, these bits represent the information indicating whether a virus check has been performed.

[0058] The fourth bit indicates whether the packet has been infected with a virus or not. If the packet has not been infected with a virus, the fourth bit is set to 0. If the packet has been infected with a virus, the fourth bit is set to 1. This signifies that the packet is the infection-indicated packet Pb. The fifth and subsequent bits represent a serial number.

[0059] Next, the warning packet Pw1 will be described.

After the virus checking router has detected a virus, the warning packet Pw1 is transmitted to the transmitting source concerned. The caution information packet Pw2 is multicast to the surrounding virus checking routers. This is intended to allow discovery of a virus at an early stage and to prevent expansion of infection with the virus.

[0060] The bits in the option field of the warning packet Pw1 are set similarly to those in a packet in which a virus is detected, and distributed to the transmitting source according to a format described below. Fig. 12 shows the format for the warning packet Pw1. First, the value specified in the IHL field is incremented by one. The copied flag bit in the option field is set to 0. The option class bits therein are set to represent 3 (field preserved for the future). The option number bits are set to represent 2 (code indicating the warning packet Pw1). The length bits are set to represent 3. The option value indicating, as described in conjunction with Fig. 11, whether a virus check has been completed or not is appended. Moreover, the end address is regarded as the address of an infecting source.

[0061] Next, processing to be performed on a client side will be described. Fig. 13 shows the configuration of the client terminal 20. The infected packet detecting means 21 employed in the present invention is included in a LAN driver 21a, and the file execution control means 22 therein is included in a TCP/IP driver 22b.

[0062] The LAN driver 21a checks a virus check bit in each packet transmitted during a data flow, and then judges whether the bit is set. The TCP/IP driver 22b is notified of the result of the judgment.

[0063] In response to the notification that the bit is set, the TCP/IP driver 22b disables execution of a file concerned and displays a message 20-1 saying that the file will be deleted.